R311 – Specific Requirements: Federal Risk and Authorization Management Program (FedRAMP)

Table of Contents

Introduction

I. Scope

This document describes the requirements for third party assessment organizations (3PAOs) seeking A2LA accreditation in the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services.

All 3PAOs seeking accreditation under FedRAMP must meet the general requirements of ISO/IEC 17020:2012.

3PAOs seeking accreditation under FedRAMP through A2LA must also meet A2LA policy and requirements documents listed below.

A 3PAO which also has an affiliated testing laboratory in information technology may apply for accreditation for its testing laboratory concurrently with its application for accreditation for FedRAMP.

II. References

- *R102f – Conditions for FedRAMP Accreditation*.
- *R105 – Requirements When Making Reference to A2LA Accredited Status*.
- *R301 – General Requirements: Accreditation of ISO/IEC 17020 Inspection Bodies*.
- *R346 – Baltimore Cyber Range Technical Proficiency Testing Activity Information*
- National Institute of Standards and Technology (NIST) Special Publication 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
- *FedRAMP Security Assessment Framework (SAF)*
- *FedRAMP System Security Plan (SSP) Template (High, Moderate, Low, LiSaaS)*
- *FedRAMP System Assessment Plan (SAP) Template*
- *FedRAMP System Assessment Report (SAR) Template*
- *FedRAMP Readiness Assessment Report (RAR) Template (High, Moderate)*
- *FedRAMP High Readiness Assessment Report (RAR) Template*
- *FedRAMP 3PAO JAB P-ATO Roles and Responsibilities*
- *FedRAMP 3PAO Obligations and Performance Standards*
- *FedRAMP 3PAO Readiness Assessment Report Guide*
- *FedRAMP General Document Acceptance Criteria*
- *FedRAMP Authorization Boundary Guidance*
- *FedRAMP Timeliness and Accuracy of Testing Requirements*
- *FedRAMP Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans*
- *FedRAMP Vulnerability Scanning Requirements*
- *FedRAMP Continuous Monitoring Strategy Guide*
- *FedRAMP Continuous Monitoring Performance Management Guide*
- *FedRAMP Significant Change Policies and Procedures*
- *FedRAMP Annual Assessment Guidance*
- *FedRAMP Annual Assessment Controls Selection Worksheet*
- *FedRAMP Penetration Test Guidance*
- *FedRAMP Agency Authorization Playbook*
- *FedRAMP Guide for Multi-Agency Continuous Monitoring*
- *FedRAMP Agency Authorization Review Report Sample Template*
- *FedRAMP New Cloud Service Offering (CSO) or Feature Onboarding Request Template*
- *FedRAMP Significant Change Form Template*
- *FedRAMP Vulnerability Scanning Requirements for Containers*

III. Definitions

3.1 For the purposes of these requirements, the relevant terms and definitions given in ISO/IEC 17000 and ISO/IEC 17020 apply.

3.2 3PAO personnel referred to in the following sections include full time, part time and contracted (i.e. 1099 contracts) individuals. All categories of personnel are expected to work within the parameters of the management system, be included in witnessing activities, and participate in the technical proficiency activity. All records of management system and technical training, along with records of witnessing and technical proficiency, shall be maintained.

IV. General Requirements

4.1 Applicant and accredited organizations under this program consent to permit A2LA to provide assessment documentation (i.e., assessor reports, checklists, etc.), corrective action plans, and any associated objective evidence of resolution of deficiencies (where applicable) to the FedRAMP Program Management Office (PMO) upon request.

4.2 The organizational chart must clearly show the functions and lines of authority for staff within the applicant's organization and the relationship, if any, between the FedRAMP security assessment functions and other activities of the applicant's organization.

4.3 3PAOs must maintain a current list of customers, which shall include all FedRAMP assessment clients. If a 3PAO is part of an organization that offers consulting services to cloud service providers (CSPs), the 3PAO must maintain a customer list for both consulting services and FedRAMP assessment services. The customer list must include all customers from the previous three years. 3PAOs must provide a copy of this list to A2LA during all annual review and renewal assessments.

4.4 To proceed with the FedRAMP PMO recognition process, the organization must be accredited to ISO/IEC 17020 under the A2LA Cybersecurity Inspection Body Program for a period of one year as evidence of implementation of the required management system.

4.5 3PAOs must meet the requirements for the technical proficiency activity, as set forth in the *R346 – Baltimore Cyber Range Technical Proficiency Testing Activity Information*.

4.6 As part of a renewal application, if a 3PAO is a Type C organization and provides consulting and/ or other cloud services for FISMA and/ or FedRAMP, the associated records may be requested as evidence of the 3PAO's understanding of the cloud consulting work. A2LA will use the evidence to help evaluate the 3PAO's understanding of FedRAMP in order to ensure the consulting services align with FedRAMP requirements. If it is determined by A2LA and/or the FedRAMP PMO that the evidence requested for the 3PAO cloud consulting work does not address FedRAMP requirements, this evidence may be grounds for revoking FedRAMP recognition.

4.7 During the A2LA assessment, the assigned assessor will ensure there is an *A2LA F337 - After Action Report for 3PAOs* completed for each assessment and the corresponding corrective actions have been recorded within the quality management system (QMS).

4.8 3PAOs have 75 days to complete any corrective actions based on deficiencies identified by A2LA during a surveillance or renewal assessment. If a 3PAO exceeds this 75 day resolution timeframe, A2LA will provide the FedRAMP PMO with a narrative of the organization's current status (i.e., still resolving 5 findings, no response provided, etc.) and the 3PAO will be designated as "In Remediation" on the FedRAMP Marketplace in accordance with the *FedRAMP 3PAO Obligations and Performance Standards*.

4.9 As part of an initial and subsequent renewal applications, 3PAOs must report any foreign ownership, control, or influence (FOCI) operations utilizing the FedRAMP 3PAO FOCI Declaration Form. If a 3PAO reports that they are under FOCI, the organization must detail how the risk is minimized or eliminated. Any changes to a 3PAO's FOCI status must be reported in the FedRAMP 3PAO FOCI Declaration Form within 48 hours following the change.

4.10 The performance management escalation process is described in the FedRAMP 3PAO Obligations and Performance Standards on www.FedRAMP.gov. Please note that if a 3PAO is revoked twice by FedRAMP, the 3PAO is no longer eligible to be recognized by FedRAMP.

V. General 3PAO Requirements

5.1 3PAOs must accommodate assessments by A2LA and/or the FedRAMP PMO when requested. "For cause" assessments are required to occur within ten business days from initial notification.

5.2 3PAO personnel participating in the FedRAMP 3PAO program must individually attest to their knowledge, understanding, and proficiency of the NIST Risk Management Framework, NIST 800-53 security controls, and FedRAMP security requirements and policies. This attestation will be captured in the *R102f – Conditions for FedRAMP Accreditation*. A2LA will assess all 3PAO candidates on this knowledge, understanding, and proficiency at the time of the A2LA assessment. The resulting artifacts (including but not limited to, the A2LA assessment package provided after each assessment) are validated and verified by the FedRAMP PMO.

5.3 A2LA accreditation is the first step in gaining FedRAMP recognition. A2LA provides evidence to the FedRAMP PMO, but that does not imply acceptance to the FedRAMP 3PAO program. A2LA submits the entire 3PAO assessment package (including the assessor report, corrective actions, correspondences and any Accreditation Council comments) to the FedRAMP PMO for final recognition. A 3PAO is not recognized by FedRAMP until the 3PAO receives an official recognition letter signed by the FedRAMP Director and is listed publicly on www.FedRAMP.gov.

5.4 If a 3PAO allows their accreditation to lapse, their FedRAMP recognition will be removed immediately, and the organization will be required to re-enter the qualification process through the A2LA Cybersecurity Inspection Body Program (see R335).

5.5 3PAOs must not submit any actual client records (i.e., SSP, SAP, SAR, etc.) to A2LA. These documents may be reviewed during the A2LA assessment, but all confidential information must remain with the 3PAO.

5.6 To ensure there are no conflicts of interest between consulting and assessing, the FedRAMP PMO reserves the right to request customer records, policies, procedures, training records, and other similar records for FedRAMP consulting services of 3PAOs who are Type C organizations. Failure to provide these records can be grounds for revoking FedRAMP recognition.

VI. ISO/IEC 17020 Additional Requirements

Additional specific requirements for this program approved by the A2LA Criteria Council are described below. The numbering system for each section below corresponds to the major sections of ISO/IEC 17020. If a section is not listed below, there are no program specific requirements in addition to what is already stated in ISO/IEC 17020.

4.1-Impartiality and Independence

4.1.3 F.1 3PAOs must ensure they do not pose a risk to their impartiality in assessing systems that will potentially house U.S. federal information. 3PAOs must ensure that all ownership, governance, personnel, finances, and payments for work align with all U.S. laws, policies, and regulations.

4.1.4 F.1 If a 3PAO reports that they are under FOCI (see Section 4.9), the 3PAO must detail how the risk is minimized or eliminated. Records of these activities shall be maintained in accordance with the FedRAMP Authorization Act.

4.1.6 F.1 3PAOs must meet the requirements of either a Type A or Type C Inspection Body as defined in ISO/IEC 17020:2012. Type B Inspection Bodies are not permitted.

4.1.6 F.2 If a 3PAO is a Type C Inspection Body, the quality of all deliverables (from both assessment and consulting services) must meet all FedRAMP quality standards as defined through the FedRAMP General Document Acceptance Criteria on www.FedRAMP.gov. Deficiencies in meeting these quality requirements may be grounds for revoking FedRAMP recognition.

5.1-Administrative Requirements

5.1.4 F.1 3PAOs must maintain appropriate insurance commensurate with the types of systems they provide assessments for and must disclose to A2LA what insurance policies they currently maintain.

5.2-Organization and Management

5.2.3 F.1 All assessments (e.g., FedRAMP Readiness, initial authorization, and annual assessments) must be staffed by an appropriate number of team members based on the complexity of the cloud system being assessed. The number of team members, for a FedRAMP High, Moderate, and Low impact initial authorization/annual assessment, must minimally consist of at least three people from the 3PAO, which includes, but is not limited to, 3PAO personnel types and their required competencies as defined in 6.1.1 F.2, 6.1.1 F.3, and 6.1.1 F.4. The number of team members, for a FedRAMP Readiness and LI-SaaS initial authorization/annual assessment, must minimally consist of at least two people from the 3PAO, which includes 3PAO personnel types and their required competencies as defined in 6.1.1 F.2 and 6.1.1 F.4. The team, as a whole, is responsible for manual control testing, penetration testing (if applicable), scanning, interviews, examination of artifacts, and report writing. During the A2LA assessment, a 3PAO must demonstrate the ability to meet the team staff requirements.

5.2.4 F.1 If a 3PAO is part of an organization that offers consulting services to CSPs, the 3PAO is not permitted to inspect a CSP system that it has provided consulting services on within the previous two years.

5.2.4 F.2 If a 3PAO is part of an organization that is also a CSP, the 3PAO is not permitted to inspect the work of their organization's CSP.

5.2.4 F.3 Tools owned or developed by a 3PAO that provide any type of direct service or support to a CSP including, but not limited to, creating FedRAMP documentation are considered a form of consulting. Therefore, to maintain the independence of an assessment, 3PAOs are not permitted to perform assessment services for the same CSP that has directly utilized tool(s) that are owned or developed by the 3PAO for any purpose. In scenarios where a tool being used is owned or developed by a company with an affiliation to a 3PAO or its management team, employees, or subcontractors, the 3PAO must document the rationale for how it maintains its impartiality from the CSP when the CSP is using the tool owned or developed by the entity affiliated with the 3PAO and how it does not infringe upon the boundaries between providing consulting and assessing services to the CSP. This rationale must be approved by both A2LA and the FedRAMP PMO.

6.1-Personnel

6.1.1 F.1 3PAOs must define the types of personnel that perform assessments activities (e.g., FedRAMP Readiness, initial authorization, and annual assessments). Each personnel type must have defined competence requirements including education, training, technical knowledge, skills and experience. These requirements shall be evidenced in a resume (or equivalent means) to demonstrate the fulfillment of the defined competencies below.

6.1.1.F.2 3PAOs must have a personnel type that is a "senior assessor" who is accountable for the overall quality of deliverables and signs off on assessments (e.g., FedRAMP Readiness, initial authorization, and annual assessments) for the 3PAO. A senior assessor must have at least five years of auditing and/or assessment experience, be a Certified Information System Security Professional (CISSP), and have at least one other industry certification from the following list:

- CompTIA Advanced Security Practitioner (CASP+) Continuing Education (CE)
- GIAC Certified Enterprise Defender (GCED)
- GIAC Certified Incident Handler (GCIH)
- GIAC Security Leadership (GSLC)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Cloud Security Professional (CCSP)
- CISSP-Information Systems Security Architecture Professional (CISSP-ISSAP)
- CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
- CISSP-Information Systems Security Management Professional (CISSP-ISSMP)
- CyberSec First Responder (CFR)
- Certified Chief Information Security Officer (CCISO)

6.1.1.F.3 3PAOs must have a personnel type that is a "penetration tester" who has the technical competence to be able to complete a penetration test in accordance with FedRAMP Penetration Test Guidance and requirements. This person must be proficient in collecting artifacts, evaluating systems/artifacts, and running penetration/security evaluation tools. A 3PAO penetration tester must have two years of penetration testing experience as the lead penetration tester and at least one industry certification related to enhancing the knowledge and skills needed to perform penetration testing activities from the following list:

- Cisco Certified Network Professional Security (CCNP Security)
- CompTIA Advanced Security Practitioner (CASP+) Continuing Education (CE)
- Certified Information Systems Security Professional (CISSP)

- Certified Secure Software Lifecycle Professional (CSSLP)
- CISSP-Information Systems Security Engineering Professional (CISSP-ISSEP)
- SANS GIAC Penetration Tester (GPEN)
- Open Web Application Security Project (OWASP) Penetration Tester
- GIAC Certified Enterprise Defender (GCED)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate-Cyber-Ops (CCNA Cyber Ops)
- Computer Hacking Forensics Investigator (CHFI)
- GIAC Certified Forensic Analyst (GCFA)
- CompTIA PenTest+

6.1.1.F.4 3PAOs must have a personnel type that is a "junior assessor" who supports the assessment activities and provides support for the quality management of the documentation. The junior assessor must have at least one industry certification from the following list:

- Cisco Certified Network Associate Security (CCNA Security)
- Cisco Certified Network Associate Cyber Security Operations (CCNA Cyber Ops)
- Cybersecurity Analyst (CySA+)
- GIAC Certified Incident Handler (GCIH)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Certified Intrusion Analyst (GCIA)
- Certified Information Systems Auditor (CISA)
- Certified Information System Security Professional or Associate (CISSP or Associate)
- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Information Systems Security Officer (CISSO)
- CyberSec First Responder (CFR)
- CompTIA Advanced Security Practitioner Continuing Education (CASP+) Continuing Education (CE)
- CompTIA Cloud+ (Cloud+)
- Global Industrial Cyber Security Professional (GICSP)
- Securing Cisco® Networks with Threat Detection Analysis (SCYBER)

6.1.2 F.1 3PAOs must have at least one person employed (not contracted or subcontracted) by the 3PAO for each personnel type identified in 6.1.1 F.1-4. A 3PAO who does not have at least one person employed (not contracted or subcontracted) for each personnel type identified in 6.1.1 F.1-4, must be approved by the FedRAMP PMO prior to recognition of the 3PAO. Exceptions are granted on a case-by-case basis and re-evaluated at each renewal assessment or if the status of the relationship changes.

6.1.2 F.2 3PAOs must maintain a relationship with any contracted or subcontracted employees for one year and must demonstrate that they are active participants in the 3PAO QMS including maintaining ongoing training requirements outlined in 6.1.5 F.1 and 6.1.5 F.2. The intention of this requirement is that a 3PAO must maintain the capability to perform a successful FedRAMP assessment while FedRAMP recognized.

6.1.5 F.1 3PAOs must develop an organizational training program for its personnel including, at a minimum, content incorporating continuing professional education (CPE) credits for FedRAMP, FISMA, cloud computing, and cybersecurity knowledge areas. Training shall comprise a minimum of 6 hours for each of the four knowledge areas mentioned above. Additionally, specific training in relation to at least one FedRAMP Authorized hyperscale system must be provided. This training program can also include industry standard certifications. 3PAOs must maintaina list of all training courses planned for the year and a statement for each item on the list as to how the training is related to these knowledge areas. The training plan must be based on the employee role in the assessment team and shall clearly delineate the intent of the plan for that individual role. The overall organizational training program will be analyzed to determine if there is sufficient technical training of assessors for understanding FedRAMP, FISMA, cloud computing, and cybersecurity.

6.1.5 F.2 All authorized 3PAO personnel must complete at least 32 hours of training annually under the training program detailed in 6.1.5 F.1. These training hours may be completed through other accreditation programs with the completion of Continuing Professional Education (CPEs) or equivalent, as long as the hours are defined adequately within 6.1.5 F.1, above. The sign off on successful completion of the CPEs is required and records shall be maintained. Also, the 32 hours of training annually is in addition to the mandatory training released by the FedRAMP PMO.

6.1.7 F.1 All authorized 3PAO personnel must register for and then complete FedRAMP-sponsored 3PAO training modules and FedRAMP-provided program update sessions within 60 days of the training and/or update announcement. All new training modules will be announced to the 3PAO's POC on file with the FedRAMP PMO. 3PAOs must maintain copies of these certificates in their training records. Records of completion will be reviewed during the A2LA assessment to ensure each team member has participated appropriately. Each individual 3PAO participant who has not completed the required training or update sessions may not participate in FedRAMP assessment activities.

6.1.10 F.1 3PAOs must maintain training records for the knowledge areas and training hours referenced in 6.1.5 F.1 and 6.1.5 F.2 for all their personnel (including subcontracted/1099 personnel) that have been involved with FedRAMP assessments for one year.

6.1.10 F.2 All training and certification records shall list the name of the organization that provided the training, the date the training occurred, and the topic of the training course.

6.1.10 F.3 3PAOs must maintain Baltimore Cyber Range participation records including participant names and pass/fail ratings.

6.2-Facilities and Equipment

6.2.1 F.1 If a 3PAO does not have a commercial facility, the 3PAO must provide justification detailing the availability, suitability, and adequacy of the facilities, equipment, and tools being used (e.g., scanning equipment, laptops, customer data tools, QMS materials, etc.).

6.2.13.b F.1 A 3PAO's procedures for protecting and securing the integrity of data (ISO/IEC 17020:2012 clause 6.2.13b) must also address collection, transmission and storage of data collected by any contracted personnel that data shall be held secure by the contracted personnel until it is transferred to the 3PAO for final review and reporting.

6.2.15 F.1 3PAOs must maintain a current security inventory list of all hardware, software, and firmware that is used by the organization to perform FedRAMP assessments. This includes patched servers for documentation collection, patched laptops for testing and gathering artifacts, and all current software used in the testing process.

6.3-Subcontracting

6.3.1 F.1 If a 3PAO subcontracts out any part of the assessment, it must ensure and be able to demonstrate that the subcontracted company is competent to perform the tasks and must comply with the relevant requirements and standards.

6.3.1 F.2 The subcontractor must be trained on the 3PAO's QMS in order to ensure compliance with ISO/IEC 17020:2012. These trainingrecords must be maintained by the 3PAO.

6.3.1 F.3 All subcontractors must also meet the same position description requirements of similar positions within the 3PAO organization.

6.3.1 F.4 3PAOs shall only subcontract as an exception to the normal course of business and must not regularly contract with clients beyond their capabilities and resources as described in ISO/IEC 17020:2012: Section 6.3 Subcontracting Note 1.

6.3.1 F.5 3PAOs must ensure that all subcontracted companies are available for any follow up actions required by FedRAMP or A2LA related to any assessment they worked on.

6.3.3 F.1 Whenever subcontracted companies perform part of the assessment, the responsibility for ensuring that all work is performed in conformance with A2LA and FedRAMP requirements must remain with the 3PAO.

7.1-Inspection Methods and Procedures

7.1.1 F.1 3PAOs must ensure that all 3PAO prescribed methods and procedures for a CSP system, align with most current NIST, DHS, and FedRAMP policies and procedures, and industry best security practices. In particular, 3PAOs must comply with all FedRAMP policies and guidance documents publicly available on www.FedRAMP.gov.

7.1.5 F.1 During the contract review process, the CSP must be informed of their ability to proactively provide feedback on the 3PAO's performance directly to A2LA and the FedRAMP PMO at any time throughout the process. The *A2LA F338 - CSP Evaluation Form* is available on the A2LA public website (www.A2LA.org) and must be provided to the CSP once the work has begun.

7.1.5 F.2 At the completion of a FedRAMP assessment, the 3PAO must inform the CSP that FedRAMP may not post their authorization on www.FedRAMP.gov until the *A2LA F338 - CSP Evaluation Form* is completed.

7.1.5 F.3 If a 3PAO has not completed a FedRAMP assessment (e.g. readiness, initial, or annual assessment) within a one year period, based on their A2LA accreditation expiration date, the 3PAO must send one representative team to participate and successfully pass the Baltimore Cyber Range Technical Proficiency Testing Activity. Non-compliance will result in the 3PAO being designated as "In Remediation" on the FedRAMP Marketplace in accordance with the *FedRAMP 3PAO Obligations and Performance Standards*.

7.4-Inspection Reports

7.4.1 F.1 3PAOs must have a documented quality review process in accordance with the *FedRAMP General Document Acceptance Criteria* for all FedRAMP deliverables.

7.4.2 F.1 All SARs written by a 3PAO must include an authorization recommendation on whether the system can appropriately safeguard government data in accordance with the security classification of the system. The recommendation shall include a summary statement and justification statement.

7.4.4 F.1 After each engagement (either readiness or full engagements), the 3PAO must create an After Action Report. The *A2LA F337 - After Action Report for 3PAOs* is available on the A2LA public website (www.A2LA.org) and must be completed within 30 days of the end of the engagement. CSPs will not be listed as FedRAMP Authorized or FedRAMP Ready on www.FedRAMP.gov until the 3PAO completes and submits the corresponding F337 online form.

8.1-Options

8.1.1 F.1 As long as a 3PAO maintains accreditation, it must continue to implement its ISO/IEC 17020:2012 management system even if they are not working on any FedRAMP engagements.

8.1.3 F.1 All 3PAO applicants will be assessed on the management system requirements listed in Section 8, Option A of ISO/IEC 17020:2012.

8.7-Corrective actions

8.7.2 F.1 3PAOs should expect to receive feedback from the FedRAMP PMO after each assessment is reviewed. 3PAOs must review the feedback and, as necessary, utilize their corrective action and complaints process. Decisions related to the feedback may result in updates to 3PAO policies, procedures, and the management system.

DOCUMENT REVISION HISTORY

Date	Description
10/15/21	➢ Minor changes to language from should to shall/must (Sections 6.1.1 F.1, 6.1.5 F.1, 6.3.1 F.4, 7.4.4 F.1) ➢ Provide clarification on annual assessment types that would preclude re-participation with Baltimore Cyber ➢ Minor updates to nomenclature for the required certifications
09/19/23	➢ Added cover page ➢ Updated section II to incorporate latest version of NIST 800-53 & NIST 800-53A ➢ Added Section 4.9 on use of FedRAMP 3PAO FOCI Declaration Form ➢ Added Section 4.10 detailing FedRAMP performance management escalation process ➢ Update to Section 4.1.4 F.1 to clarify expectations based on the FedRAMP Authorization Act ➢ Clarified the definition of FedRAMP assessments throughout ➢ Updated links to F337 and F338 forms throughout ➢ Added additional approved certifications for penetration testers to Section 6.1.1.F.3 ➢ Added "and certification" to Section 6.1.10.F.2 ➢ Clarified responsibilities for After Action Report in Section 7.4.4.F.1